# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-184643
(43)Date of publication of application : 01.07.1992

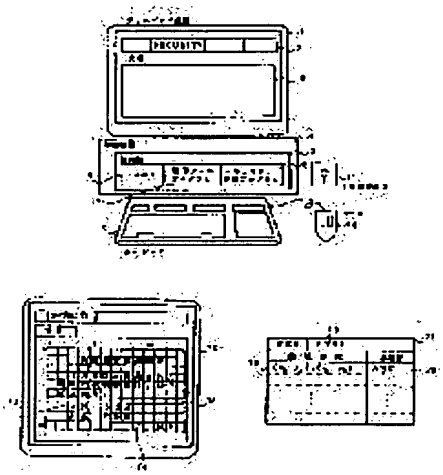
(51)Int.Cl. G06F 12/00
G06F 15/20
G09C 1/00

(21)Application number : 02-315615
(22)Date of filing : 20.11.1990

(71)Applicant : HITACHI LTD
(72)Inventor : NAKAMURA HIROAKI
KIRIKOSHI SHINICHI
KAJIWARA TAKEMASA

## (54) PROTECTING METHOD FOR ELECTRONIC DOCUMENT

(57)Abstract:
PURPOSE: To reject the accesses given from the persons except a due approver by designating an optional secret protection area of an electronic document including the secret areas and also the information on the access approver assigned to the designated area, turning these designated information into a table, and referring to this table when an access is confirmed.
CONSTITUTION: It is checked whether an area to be protected is included in a produced document 12 or not. If so, a security control program 8 is called with a function key of a keyboard 9 or a security item is picked up out of the guidance column of a display device 1 with a mouse 10. Then an area covering the head character 13 through the final character 14 is designated with the keyboard 9 or the mouse 10 in a specific area where the accesses of the outsiders are not approved. This designated range is set to a security information table 21. At the same time, the characters included in a designated area of a memory 6 are ciphered and rewritten into the different codes. Then a mask is applied to the designated area of the device 1. If the information on an approver who can have an access to the designated area is received, this information is set an approver column 20.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−184643

| ⑤Int.Cl.⁵ | 識別記号 | 庁内整理番号 |
|---|---|---|
| G 06 F 12/00 | 537 H | 8944−5B |
| 15/20 | 586 J | 6945−5L |
| G 09 C 1/00 | | 7922−5L |

⑬公開　平成4年(1992)7月1日

審査請求　未請求　請求項の数 6　(全11頁)

⑭発明の名称　電子文書の保護方法

⑳特　願　平2−315615

㉒出　願　平2(1990)11月20日

㉗発明者　中村　博暁　神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内

㉗発明者　桐越　信一　神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内

㉗発明者　梶原　孟正　神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内

㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地

㉔代理人　弁理士　磯村　雅俊

## 明細書

1．発明の名称

電子文書の保護方法

2．特許請求の範囲

1．機密個所を有する電子文書中の任意の機密保護領域を指定し、該機密保護指定領域に対するアクセス承認者に関する情報を設定することにより、前記機密保護指定領域を暗号化して保管するとともに、前記機密保護指定領域に対する前記アクセス承認者以外からのアクセスを防止することを特徴とする電子文書の保護方法。

2．前記機密保護指定領域に対する前記アクセス承認者に関する情報を電子文書情報に付随させることを特徴とする請求項1記載の電子文書の保護方法。

3．前記機密保護指定領域に対する前記アクセス承認者以外からのアクセスに対しては、前記機密保護指定領域についてはマスクしたまま出力することを特徴とする請求項1記載の電子文書の保護方法。

4．機密個所を有する電子文書に関して利用者を限定してアクセス権限を定め、該アクセス権限情報を電子文書情報に付随させることにより、前記電子文書に対する前記アクセス権限以外のアクセスを防止することを特徴とする電子文書の保護方法。

5．前記利用者を限定して定められたアクセス権限情報を、電子文書情報に付随させて送受信することにより、受信元での、前記機密保護指定領域に対する前記アクセス承認者以外からのアクセスを防止することを特徴とする請求項4記載の電子文書の保護方法。

6．機密個所を有する電子文書中の任意の機密保護領域を指定し、また、該機密保護指定領域に対するアクセス承認者に関する情報を設定し、前記機密保護指定領域を暗号化するとともに、前記アクセス承認者に関する情報を電子文書情報に付随させて送受信することにより、受信元での、前記機密保護指定領域に対する前記アク

セス承認者以外からのアクセスを防止することを特徴とする電子文書の保護方法。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は電子文書の保護方法、すなわち、機密個所を有する電子文書の不法な複写や、第三者からのアクセス防止に有効な電子文書における任意の指定領域の保護方法、および、機密個所を有する電子文書内の重要機密個所の不法な複写や、第三者からのアクセス防止に有効な電子文書における任意の指定領域の保護方法に関する。

〔従来の技術〕

従来のこの種の方法としては、例えば、日立クリエイティブワークステーション2050，ＯＦＩＳ/ＤＥＳＫ-ＥＶ(2)(日立製作所，平成元年9月刊)に記載されている如く、文書情報について更新や参照等の可，不可属性を与え、文書全体に対しての保護を可能としているものがある。これによれば、文書情報の不法な複写や第三者からのアクセス防止を行うことができる。

〔発明が解決しようとする課題〕

上記従来技術では、文書の作成者とこれを利用する使用者とを区分して、アクセス権限を定めることにより、文書全体に対しての機密保護を行うことは可能であるが、特定の部分、つまり重要機密事項部分を任意に指定して、ここだけを機密保護の対象とすることはできなかった。

また、上記従来技術では、例えば、重要文書に特定の人(上司等)の承認印(サイン)をもらう場合の如く、利用者を限定してアクセス権限を定めるという点については配慮されていなかった。

更に、上記従来技術では、機密個所を有する電子文書を電子メール等の手段で送信する際に、上述の如き重要機密事項部分の保護機能や、特定の人に対するアクセス権限の指定を含めて送信するという点についても配慮されていなかった。すなわち、上記従来技術では、機密個所を有する電子文書を、電子メール等の方法により、機密保護状態を有するまま送受信するという点については配慮されていなかった。

本発明は上記事情に鑑みてなされたもので、その目的とするところは、従来の技術における上述の如き問題を解消し、機密個所を有する電子文書の特定部分のみを保護対象とすることが可能な電子文書の保護方法を提供することにある。また、本発明の他の目的は、機密個所を有する電子文書に対して、利用者を限定してアクセス権限を定めることが可能な電子文書の保護方法を提供することにある。本発明の更に他の目的は、機密個所を有する電子文書を、機密保護状態を有するまま送受信することを可能にする電子文書の保護方法を提供することにある。

〔課題を解決するための手段〕

本発明の上記目的は、機密個所を有する電子文書中の任意の機密保護領域を指定し、該機密保護指定領域に対するアクセス承認者に関する情報を設定することにより、前記機密保護指定領域を暗号化して保管するとともに、前記機密保護指定領域に対する前記アクセス承認者以外からのアクセスを防止することを特徴とする電子文書の保護方法によって達成される。本発明の他の目的は、機密個所を有する電子文書に関して利用者を限定してアクセス権限を定め、該アクセス権限情報を電子文書情報に付随させることにより、前記電子文書に対する前記アクセス権限以外のアクセスを防止することを特徴とする電子文書の保護方法、および、機密個所を有する電子文書中の任意の機密保護領域を指定し、また、該機密保護指定領域に対するアクセス承認者に関する情報を設定し、前記機密保護指定領域を暗号化するとともに、前記アクセス承認者に関する情報を電子文書情報に付随させて送受信することにより、受信元での、前記機密保護指定領域に対する前記アクセス承認者以外からのアクセスを防止することを特徴とする電子文書の保護方法によって達成される。

〔作用〕

本発明に係る第1の電子文書の保護方法においては、機密個所を有する電子文書中の任意の機密保護領域を指定可能とし、また、該機密保護指定領域に対するアクセス承認者に関する情報を設定

可能としてこれらの情報をテーブル化しておき、アクセスがあった場合に上述のテーブルを参照して、機密保護指定領域に対するアクセスが上記アクセス承認者以外からのアクセスである場合には上記機密保護指定領域へのアクセスを実質的に拒否するようにしたものである。

本発明に係る第2の電子文書の保護方法においては、機密個所を有する電子文書に関して利用者を限定してアクセス権限を定め、このアクセス権限情報をテーブル化して電子文書情報に付随させておくことにより、当該電子文書に対する利用者とそのアクセス権限に関する情報を不可分にしたものである。

本発明に係る第3の電子文書の保護方法においては、機密個所を有する電子文書中の任意の機密保護領域を指定可能とし、また、この機密保護指定領域に対するアクセス承認者に関する情報を設定可能として、機密保護指定領域を暗号化するとともに、上述のアクセス承認者に関する情報を電子文書情報に付随させて送受信することにより、受信元での、機密保護指定領域に対するアクセス承認者以外からのアクセスを防止するようにしたものである。

〔実施例〕

以下、本発明の実施例を図面に基づいて詳細に説明する。

第2図は、本発明の一実施例である文書処理装置の構成を示す図である。図中、1はディスプレイ装置、4は制御装置、9はキーボード、10はマウスを示している。ディスプレイ装置1はガイダンス欄2と文書入力部3から構成されており、制御装置4は装置全体を制御する制御部5に、ワークステーション等で処理する場合に、文書データやプログラムの記憶場所となるメモリ6と、電子メールの送受信を制御する電子メールプログラム7、更には、保護指定領域の範囲やアクセスを認める承認者情報の暗号化、マスク化等、指定領域の保護に関する処理を制御するセキュリティ制御プログラム8が組み込まれた構成となっている。また、キーボード9は文字やカーソル位置を入力する機能を有するもの、マウス10は机上で動かして画面上のカーソルの動きを指示する機能を有するもの、文書保管媒体11は文書を格納する機能を有するものである。

第3図は、作成された文書12内の重要機密部分の例を示す図で、第三者にアクセスされたくない部分を、先頭点13から終点14で示した例である。

また、第4図は、上述の第三者にアクセスされたくない部分(第3図の15)が保護され、マスク化(16)された状況を示す文書例(17)である。

第5図は、文書内の指定領域範囲19およびその領域内のアクセスを認める承認者情報20を登録するためのセキュリティ情報テーブル21の構成例を示すものであり、文書の最後部に作成され、文書と連動するようになっている。

第6図は、文書内の保護指定領域のアクセスを認める承認者情報を入力するセキュリティ情報入力ガイダンスである。

第7図は、文書を保管する媒体の内部構成例を示すものである。文書保管媒体は、図に示される通り、媒体管理領域22，ディレクトリ領域23およびファル領域24から構成されており、媒体管理領域22は、ディレクトリ領域23とファル領域24の位置や大きさ等、媒体全体を管理する領域である。ディレクトリ領域23は、文書名，所有者名およびセキュリティ情報テーブル21の位置等の、ファイル領域24に関する情報を管理しており、ファイル領域24は、文書データを格納するテキスト部25とセキュリティ情報が格納されているテーブルの属性格納部26から構成されている。

第1図は、本実施例における任意の指定領域保護方法を実現する処理フローチャートである。以下、第1図を基に、第2図～第7図をも用いて、本実施例の動作を説明する。

まず、第2図に示したシステム装置で、第3図に示すような文書12を作成する(ステップ 700)。次に、作成した文書内の保護する領域があるか否かをチェックし(ステップ 701)、ある場合には、セキュリティ制御プログラム8を、キーボード9のファンクションキーか、ディスプレイ装置1の

ガイダンス側のセキュリティ項2を、マウス10でピックする等して呼び出す(ステップ 702)。

ステップ 703では、文書内の機密事項で、第三者からのアクセスを認めない特定領域の先頭文字13から、最終文字14までの範囲を、キーボード9あるいはマウス10で指定する。これにより、セキュリティ制御プログラム8は、セキュリティをかける領域の先頭点($x_a$, $x_a$)、最終点($x_b$, $x_b$)を検出して、これをセキュリティ情報テーブル21にセットする(ステップ 704)と同時に、メモリ6内の指定領域内文字を、暗号化で別コードに書き換え(ステップ 705)、ディスプレイ装置1上の指定領域にマスクをかける(ステップ 706)。

次に、ステップ 707で、セキュリティ制御プログラム8は、第6図に示したセキュリティ情報入力ガイダンスをディスプレイ装置1上に表示し、アクセスを認める承認者情報をキーボード9から入力させ、これをセキュリティ情報テーブル21の承認者欄20にセットする(ステップ 708)。なお、この承認者情報も、ステップ 709において、暗号化し別コードに書き換える。指定領域が複数ある場合には、上述のステップ 702～ステップ 709を繰り返す。

第7図に、作成した文書をフレキシブルディスク(ＦＤ)や内蔵ディスク等の文書保管媒体に格納したときの媒体内のフォーマットを示している。ステップ 711では、文書指定領域保護処理終了がキーボード9またはマウス10から入力された場合に、文書名、文書所有者名、文書の大きさ等、文書全体を管理する情報を第7図のフォーマット中のディレクトリ領域23、文書をテキスト部25、また、セキュリティ情報テーブル21を属性格納部26として、媒体に保管し終了する。なお、この際、上述の保護をかけてある領域の文字は、当然、暗号化で変換された解読不能文字のままで媒体に保管する。

第8図は、電子メールでの文書送信処理のフローチャート、第9図は、電子メールでの文書受信処理と保護領域の表示処理のフローチャート、また、第10図は、電子メールで文書を送受信するときの処理概要図である。第10図においては、受信側にセキュリティ制御プログラム8がある場合とない場合、更には、指定領域に所有者が付加したセキュリティ情報と、利用者が入力した情報とが一致した場合と一致しない場合の表示方法の違いを示すものである。

まず、第8図に基づいて、送信時の動作を説明する。

第4図の如く作成し、文書指定領域保護処理が終了した文書を電子メールで送信する場合、電子メールプログラム7を呼び出し(ステップ 800)、そのプログラムが出力するメール送信ガイダンス28(第10図参照)に従って、文書名29、あて先名30を入力させる(ステップ 801)。電子メールプログラム7は、送信する文書の属性から、保護されている領域があるか否かを判断し、第11図に示す、ヘッダ部42とテキスト部43で構成される伝送データ41のヘッダ部42内に、セキュリティ属性フラグ47を自動的に付加して(ステップ 802)、伝送データを作成し(ステップ 803)、第10図に示す接続ホスト32を経由して、相手側のメールボックス34へデータを伝送する(ステップ 804)。

次に、第9図に基づいて、文書の受信時の動作を説明する。

メール受信側33では、送られてきた文書名を指定する(ステップ 900)。これにより、メールボックス34からメモリ37内へ伝送データ41が読み込まれる(ステップ 900)。この受信側にはセキュリティ制御プログラムがあるので、ステップ 902からステップ 903に進み、そのセキュリティ制御プログラムにより、伝送データ41中のセキュリティ属性フラグ47がＯＮかＯＦＦかをチェックする。ＯＦＦの場合には、保護されていないとみなし、文書全体を表示する(ステップ 911)。

また、セキュリティ属性フラグ47がＯＮの場合には、メモリ内で伝送データ41中のテキスト部43を、文書48とセキュリティ情報テーブル49とに分割し(ステップ 904)、セキュリティ情報テーブル49の領域情報19から得た保護領域をマスク化した状態(第4図17参照)でディスプレイ装置に表示す

る(ステップ 805)。次に、セキュリティ制御プログラムは、第10図に示す利用者情報入力ガイダンス35を出力し、利用者にこれに従ってユーザＩＤ等の利用者情報を入力させる(ステップ 806)。

ここで、利用者が入力した承認者情報が、所有者が指定したセキュリティ情報テーブル内の情報と一致しすれば(ステップ 807)、セキュリティ制御プログラムは、暗号化された情報を通常の文書に変換し、マスクを解除して、ディスプレイ装置に表示する(ステップ 808と809)。なお、この際、保管媒体上の文書データは、暗号化されたままである。また、ステップ 806で、利用者が入力した承認者情報が、所有者が指定したセキュリティ情報テーブル内の情報と一致しない場合には、セキュリティ制御プログラムは、エラーメッセージを出力し(ステップ 812)、表示動作を中止する。

また、メールのあて先間違い等で、メール受信側にセキュリティ制御プログラムがない装置に文書を送信してしまい、受信者(第10図の38)がメールボックス38からメモリ40に読み込み、表示しようとした場合には、指定領域情報は暗号化されたデータのままで(マスク化されない状態で)ディスプレイ装置に表示される。更に、文書の最後部にあるセキュリティ情報テーブル内の情報も、テキスト部の一部であるため表示されるが、この情報も利用者からは解読不能である(ステップ 810)。

上記実施例によれば、文書内の指定領域を暗号化することで、文書保管媒体の盗難時等や、電子メールのあて先間違い時における文書内重要情報の漏出防止や機密保護が可能となり、第三者による不法な複写やアクセス防止等、機密管理の強化が達成できる効果がある。

次に、本発明の他の実施例を示す。

第12図は、文書内の指定領域を保護するために必要となる文書名50，指定領域範囲51，その領域内のアクセスを認める承認者情報52と領域内の参照権，更新権等を決定するアクセス権限情報53を登録するセキュリティ情報テーブル54を示すものである。本テーブルは、前述の如く、文書の最後部に作成され、電子メール等で送受信される場合には、文書と同様の動作をするものである。

第13図は、上述の保護指定領域のアクセスを認める承認者情報52と指定領域についてのアクセス権限情報53を入力するための、セキュリティ情報入力ガイダンスを示すものである。

第14図は、指定領域に対して、参照できるか、更新できるか等のアクセス権限を付加する処理のフローチャートであり、以下、これに基づいて、アクセス権限付加処理の動作を説明する。

まず、第２図に示したシステム装置で、文書を作成する。次に、作成した文書の保護指定領域に対し、アクセス権限を付加する文書名を入力する(ステップ1401)ことで、メモリ内に文書が読み込まれ(ステップ1402)、アクセス権限を付加する場合(ステップ1403)、セキュリティ制御プログラムを、キーボード９のファンクションキーか、ディスプレイ装置１のガイダンス欄２を、マウス10でピックする等して呼び出す(ステップ1404)。

次に、前述の実施例と同様に、文書内の保護指定領域の先頭と最終文字を指定することで、保護指定領域をセキュリティ情報テーブルにセットする。更に、第13図に示したセキュリティ情報入力ガイダンスを出力し(ステップ1405)、利用者がこれに従って、アクセス承認者に対して、その領域の更新権58，参照権59あるいはアクセス不可60を入力する(ステップ1406)ことで、セキュリティ制御プログラムは、セキュリティ情報テーブル54にアクセス権限情報をセットする(ステップ1407)。アクセス権限を付加する領域が複数ある場合は、上述のステップ1404～ステップ1407を繰り返す。

第15図に，アクセス権限が付加されている文書を電子メールで送受信し、アクセス権限の付加状態に基づく指定領域の参照，更新等の処理動作のフローチャートを示した。以下、これに従って動作を説明する。なお、スタート(文書名入力)から利用者が承認者情報入力ガイダンスに従って承認者情報を入力するまでの動作は、第９図のステップ 801～ステップ 806と同じであるので、詳細な説明は省略する。

利用者が入力した承認者情報とセキュリティ情

報テーブル54内の承認者情報52とが一致している場合には(ステップ1502)、上述のセキュリティ情報テーブル54内の更新ビット61，参照ビット62，アクセス不可ビット63がＯＮＯＦＦかをチェックする(ステップ1503，同1504)。更新ビット61がＯＮの場合は、指定領域内の暗号化，マスク化を解除し(ステップ1508)、その領域内の参照，更新が可能になる(ステップ1509)。更新ビット61がＯＦＦで、参照ビット62がＯＮの場合は、指定領域内の暗号化，マスク化を解除し(ステップ1506)、その領域内の情報を表示する(ステップ1507)。しかし、この場合は、表示のみであり、その領域内への書き込みはできない。

また、更新ビット61と参照ビット62がＯＦＦの場合、すなわち、セキュリティ情報テーブル54内のアクセス不可ビットがＯＮの場合には、指定領域内の情報はマスク化された状態でディスプレイ装置に表示され、指定領域の参照，更新はすることができない(ステップ1505)。

上記実施例によれば、文書内の保護指定領域にアクセス権限を付加したことにより、保護指定領域に対しては、承認された外だけがアクセスできるようになり、例えば、重要文書の承認サインをもらう場合、電子メールで文書を送り、それに対しての回答や意見等を求める場合に、利用者の限定が可能になり、しかも、その領域に対する第三者からの不法な書き込み等のアクセスを防止できるという効果が得られる。

上記実施例は本発明の一例を示すものであり、本発明はこれに限定されるべきものではないことは言うまでもない。

〔発明の効果〕

以上、詳細に説明した如く、本発明によれば、機密個所を有する電子文書の特定部分のみを保護対象とすることが可能な電子文書の保護方法，および、機密個所を有する電子文書に対して、利用者を限定してアクセス権限を定めることが可能な電子文書の保護方法，機密個所を有する電子文書を、機密保護状態を有するまま送受信することを可能にする電子文書の保護方法を実現できるという顕著な効果を奏するものである。

4．図面の簡単な説明

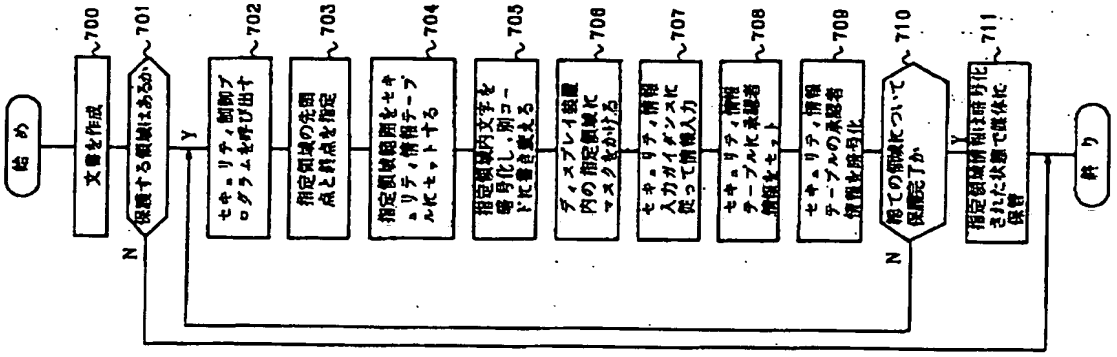
第１図は本発明の一実施例における指定領域保護方法を実現する処理フローチャート、第２図は実施例の文書処理装置の構成を示す図、第３図は作成された文書内の重要機密部分の例を示す図、第４図は第三者にアクセスされたくない部分が保護され状況の文書例を示す図、第５図はセキュリティ情報テーブルの構成例を示す図、第６図はセキュリティ情報入力ガイダンスを示す図、第７図は文書を保管する媒体の内部構成例を示す図、第８図は電子メールでの文書送信処理のフローチャート、第９図は電子メールでの文書受信処理と保護領域の表示処理のフローチャート、第10図は電子メールで文書を送受信するときの処理概要図、第11図は伝送データの構成例を示す図、第12図は本発明の他の実施例におけるセキュリティ情報テーブルの構成例を示す図、第13図はセキュリティ情報入力ガイダンスを示す図、第14図はアクセス権限付加処理のフローチャート、第15図はアクセス権限が付加されている文書の電子メールでの送受信処理と指定領域の参照，更新等の処理動作のフローチャートである。

１：ディスプレイ装置、２：ガイダンス欄、３：文書入力部、４：制御装置、５：制御部、６：メモリ、７：電子メールプログラム、８：セキュリティ制御プログラム、９：キーボード、10：マウス、11：文書保管媒体、15：文書内の新定指定領域、21および54：セキュリティ情報テーブル。

代理人　弁理士　最　村　雅　俊

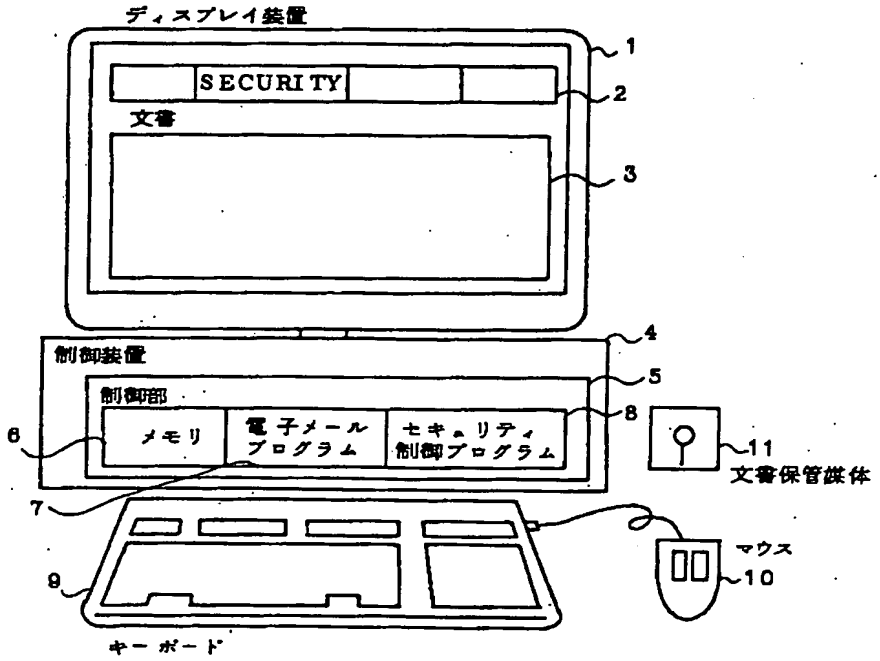
第1図

指定領域保護処理フロー



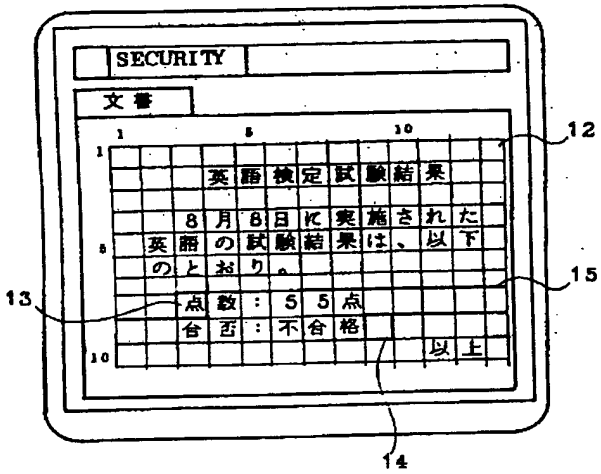

第2図

システム装置



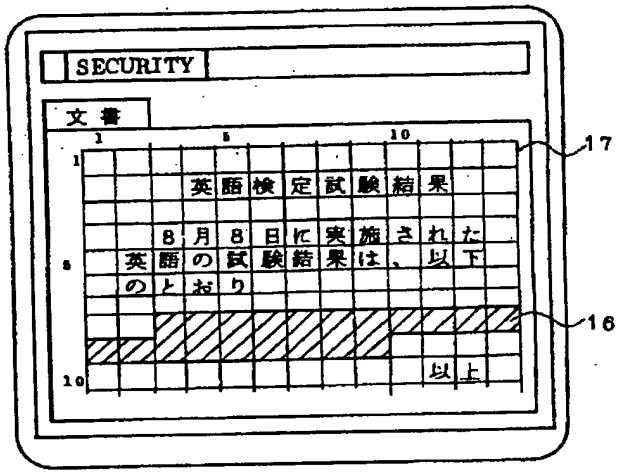
第 3 図

指定領域の範囲指定例



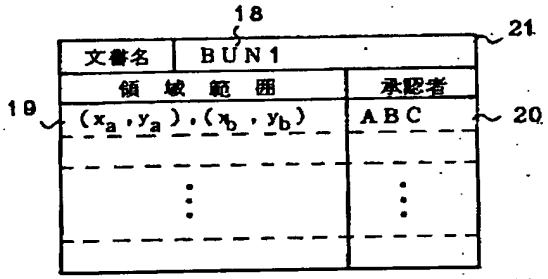

第 4 図

保護，マスク化された例



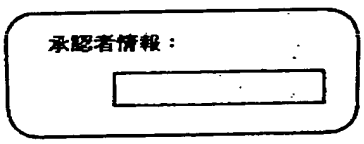

第 5 図

セキュリティ情報テーブル



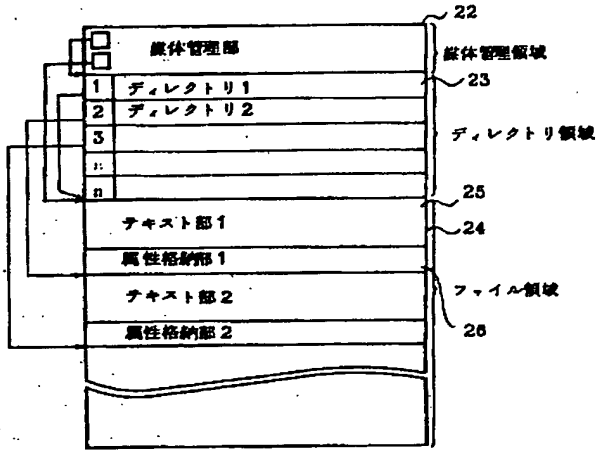

第 6 図

セキュリティ情報入力ガイダンス



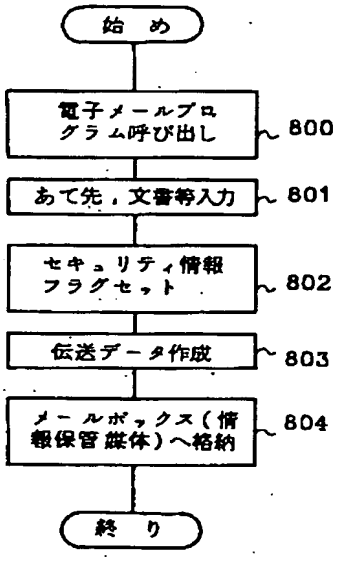

第 7 図

文書保管媒体構成図



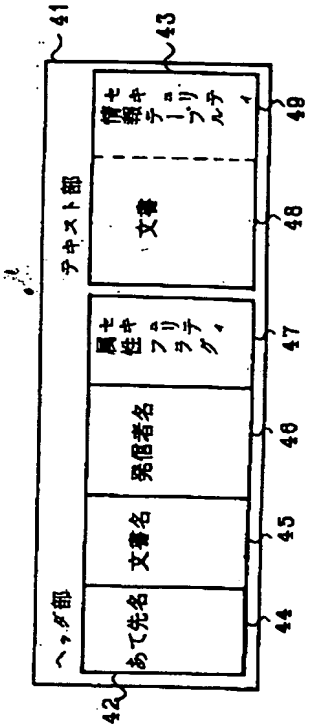
第 8 図

電子メールでの文書送信処理フロー



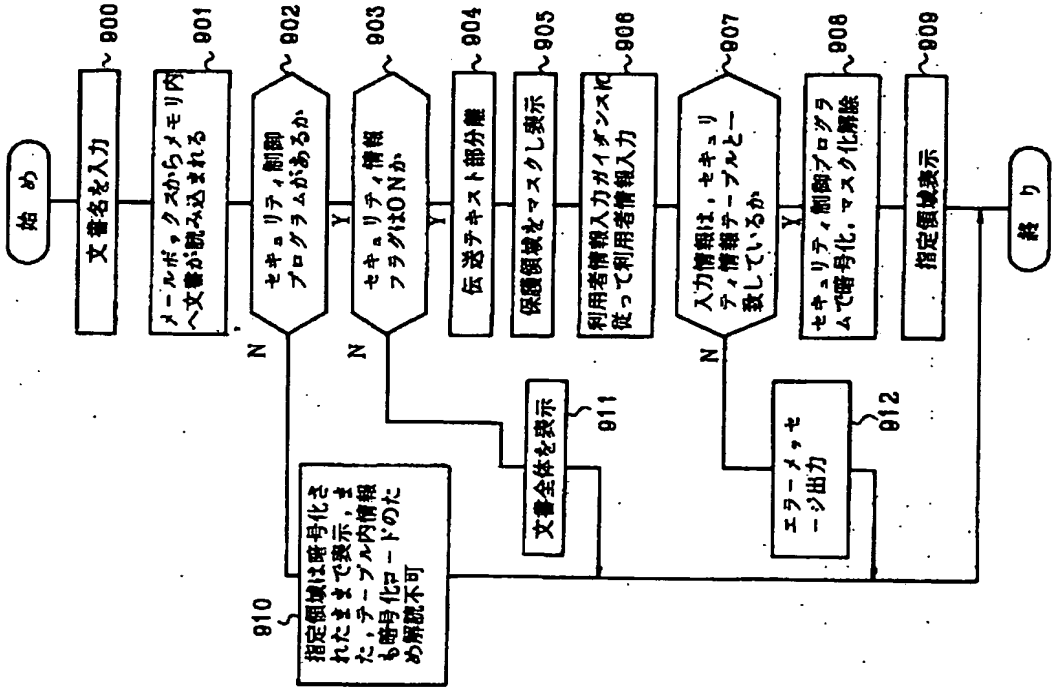

第 11 図

伝送データ形式



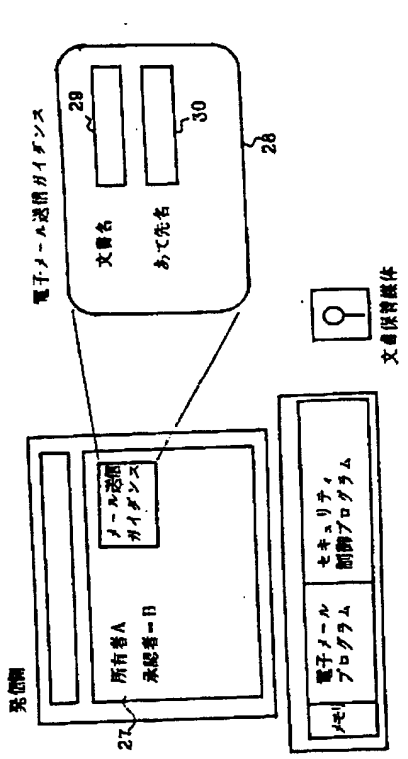

第 9 図

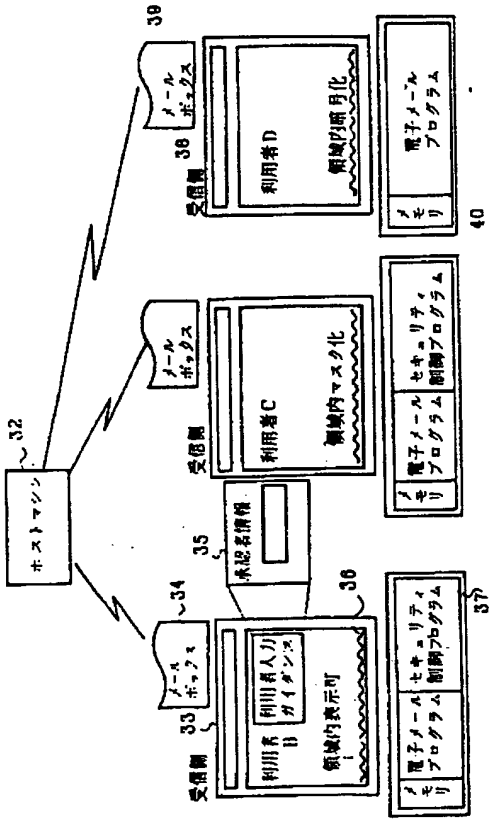
電子メールでの受信と表示処理フロー



第 10 図

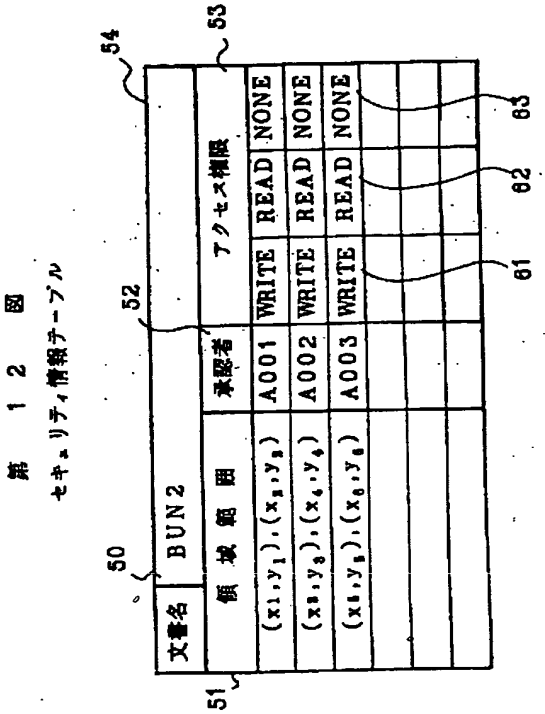
電子メール送受信処理概要



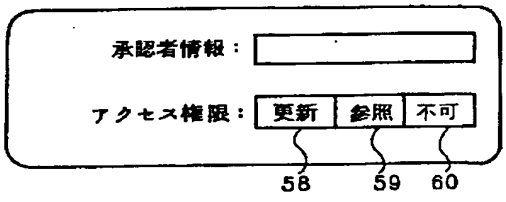

第 12 図

セキュリティ情報テーブル



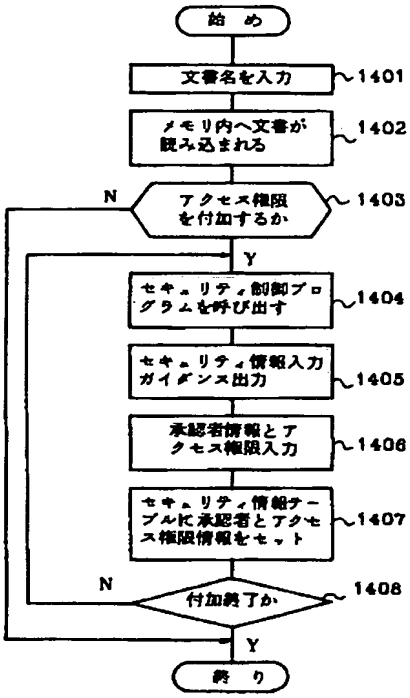

第 13 図

セキュリティ情報入力ガイダンス



第　14　図

アクセス権限付加処理フロー




第　15　図

電子メールアクセス権限処理フロー